IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

ContentGuard Holdings, Inc., Plaintiff, -against- Google, Inc. Defendant.	Civil Action No. 2:14-cv-00061-JRG JURY TRIAL DEMANDED
ContentGuard Holdings, Inc., Plaintiff, -against- Amazon.com, Inc., *et al*. Defendants.	Civil Action No. 2:13-cv-01112-JRG JURY TRIAL DEMANDED

PLAINTIFF CONTENTGUARD HOLDINGS, INC.'S RESPONSE TO DEFENDANTS' RENEWED MOTION FOR JUDGMENT ON THE PLEADINGS

TABLE OF CONTENT

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

I. INTRODUCTION

Defendants' renewed motion for judgment of invalidity pursuant to 35 U.S.C. § 101 ("Section 101") fails to cure the fatal flaws that plagued Defendants' previous motions seeking the same relief. Defendants continue to trivialize and mischaracterize ContentGuard's seminal inventions by, among other things, inviting the Court "look[] past" their "complexity." *Amazon* Action Dkt. 539 at 1.[1] Defendants also continue to assert that ContentGuard's technology-based inventions are ineligible for patent protection because they allegedly are analogous to "conventional" practices implemented through manual processes and honor codes (*e.g.*, library cards, unenforceable promises, background checks, etc.).

At bottom, Defendants' methodology is one of deconstruction—Defendants reduce the inventions to their atomic sub-parts and then pretend that each of those sub-parts is "conventional" because it resembles, however slightly, pre-existing activities. The fundamental fallacy here is that, if Defendants' methodology were correct, Section 101 is certain to "swallow all of patent law." *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S. Ct. 2347, 2354 (2014) (citations and internal punctuation omitted). Indeed, no patent is safe from the type of "analysis" espoused by Defendants because every patent can be caricatured to the point where it is "analogous" to a practice that is "conventional" and "pre-existing." But because, as the Supreme Court explained in *Alice Corp.*, "at some level, all inventions . . . embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas," *id.*, that is precisely how the analysis is *not* supposed to be conducted.

Properly considered, all of the inventions at issue in this litigation are eligible for patent protection, as demonstrated herein. Defendants' motion should be denied.

II. RELEVANT BACKGROUND

Consistent with their strategy of ignoring and misrepresenting the actual inventions

[1] The defendants in the *Amazon* and *Google* action filed a consolidated motion. For the sake of simplicity we cite herein only to the motion filed in the *Amazon* action under Dkt. 539.

taught by the patents-in-suit, Defendants carefully avoid making any mention of these inventions' background. Because "the determination of patent eligibility requires a full understanding of the basic character of the claimed subject matter," *Bancorp Servs., L.L.C. v. Sun Life Assurance Co. of Canada (U.S.)*, 687 F.3d 1266, 1273-74 (Fed. Cir. 2012), we provide the missing context below.

A. The Trusted Repository ('859, '576, '072, '956, 007, and '160) Patents

In the early 1990s the research-oriented Advanced Research Projects Agency Network, aka ARPANET, was undergoing its transition to become the first public Internet.[2] It was apparent at the time that the Internet was going to fundamentally alter the way in which digital content would be offered to and accessed by consumers, but there was enormous skepticism that the owners of content could continue to protect the fruits of their labor. Exs. 3, 5. Because the Internet was perceived as "a pirate's paradise," "the instant and practically costless copying and distribution the Net facilitates ha[d] made many creators, authors, and copyright-holders balk at digitizing and posting their ideas." Ex. 5. John Perry Barlow, a well-known commentator and a co-founder of the Electronic Frontier Foundation, summarized the challenge as follows:

> If our property can be infinitely reproduced and instantaneously distributed all over the planet without cost, without our knowledge, without its even leaving our possession, how can we protect it? How are we going to get paid for the work we do with our minds? And, if we can't get paid, what will assure the continued creation and distribution of such work? *Since we don't have a solution to what is a profoundly new kind of challenge, and are apparently unable to delay the galloping digitization of everything not obstinately physical, we are sailing into the future on a sinking ship*.

Ex. 3 (emphasis added).

Determined to find a solution that would ignite Internet-based commerce in digital content, a small team of scientists working at Xerox's Palo Alto Research Center ("PARC") set out to solve Barlow's "immense, unsolved conundrum." *Amazon* Action Dkt. 244 ¶ 4. Led by Mark Stefik, the PARC team began to explore technical solutions that would not only prevent

[2] *See* http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

piracy, but would also enable musicians, authors, photographers, publishers, and producers to share, track, control, and monetize their content. *Id.* Through a series of revolutionary inventions, Stefik and his colleagues Peter Pirolli and Ralph Merkle laid the technological foundation for what would ultimately become the prevailing paradigm for securely distributing digital content over the Internet. *Id.* In November 1994, realizing the potential unlocked by Stefik and his colleagues' work, PARC sought patent protection for their digital management rights ("DRM") innovations.

Because they "cover much of what we'd [today] describe as digital rights management," Stefik's patents are complex. Ex. 2. Of special significance here, however, is a particular aspect of Stefik's innovations, specifically their teachings concerning "trusted" systems. At bottom, Stefik's vision was that "trusted systems . . . would be the only feasible way to implement digital rights management because general-purpose computers ha[d] too many security holes." Ex. 6. As described at length in Stefik's Trusted Repository Patents (*Amazon* Action Dkt. 244-03 ('859 Patent) at cols. 12-13), a key feature of such "trusted" systems is reflected in the requirement that they maintain three types of "integrities"—physical, communications, and behavioral—in the support of usage rights that are associated with the content. As envisioned by Stefik and as construed by the Court, a "trusted" system (1) prevents access to information by a non-trusted system; (2) ensures that it only communicates with other devices that are able to present proof that they are trusted systems, for example, by using security measures such as encryption, exchange of digital certificates, and nonces; (3) requires software to include a digital certificate in order to be installed in the repository.

Stefik's "pioneering" work with respect to "trusted" systems has received numerous accolades. Ex. 7. As commentators have noted, Stefik's vision concerning the role "trusted" systems must play in the distribution of digital content over the internet is one of the seminal "development[s] that catalyzed the DRM paradigm." Ex. 6. "Trusted" systems are now firmly considered a "core technolog[y] that underlie[s] . . . technological protection systems" (*id.*), and

Stefik is "acknowledged [as the] father of DRM" (Ex. 1). Along the same lines, Stefik's Trusted Repository Patents have been praised as disclosing fundamental technology "*necessary* to make the digital delivery of music, movies and other files secure." Ex. 8 (emphasis added). Indeed, when Microsoft Corporation sought to acquire a controlling interest in ContentGuard,[3] the EU antitrust authorities threatened legal action out of concern that Microsoft could use ContentGuard's patents to suppress competition. Ex. 2.

Four of the six Trusted Repository Patents at issue in this action were recently challenged before the PTAB in *Inter Partes* Reviews. Ex. 9. Since its founding, the PTAB has been extraordinarily uncharitable to patent holders, prompting the former Chief Judge of the Federal Circuit to liken this institution to a "death squad[]" on a mission to "kill[intellectual] property rights." Ex. 10. The PTAB, however, reaffirmed the validity of each and every claim at issue in these patents,[4] distinguishing the challenger's asserted prior art on the basis that it did not disclose Stefik's "trusted" repository limitations. Ex. 11.

B. The Meta-rights ('280 and '053) Patents

ContentGuard's Meta-rights Patents build upon the innovations taught by the Trusted Repository Patents. Recognizing that "business models for creating, distributing, and using digital content and other items involve a plurality of parties," *i.e.*, content creators, publishers, distributors, and end-users (*Amazon* Action Dkt. 244-05 ('280 Patent) at col. 2:24-26), and that parties residing upstream in the distribution chain may wish to exercise "control over downstream parties" (*id.* at col. 2:33-34), the inventors of the '280 and '053 Patents invented the concept of "meta-rights . . . enforceable by a repository." The '280 and '053 Patents define "meta-rights" as "the rights that one has to generate, manipulate, modify, dispose of or otherwise derive other rights." *Id.* at col. 5:45-47. Unlike the "usage rights" taught by the Trusted

[3] As explained in the Second Amended Complaint, ContentGuard was formed in 2000 as joint venture between Microsoft and Xerox. *Amazon* Action Dkt. 244 ¶ 5.
[4] With respect to the '160 Patent, the PTAB declined to institute a review concerning the claims at issue in these litigations.

Repository Patents, whose exercise result in "actions to content" (*id.* at col. 7:26-27), "[w]hen meta-rights are exercised, new rights are created from the meta-rights or existing rights are disposed as the result of exercising the meta-rights" (*id.* at col. 7:28-31). No "actions to content," however, result from the exercise of meta-rights.

The claims of the Meta-rights Patents recite "repository" limitations and expressly incorporate the Trusted Repository Patents' teachings concerning trusted repositories. Thus, to ensure that the entirety of the content distribution chain maintains its integrity, the Meta-rights Patents require that "meta-rights" be "enforceable by a repository." *See Amazon* Action Dkt. 244-05 ('280 Patent) claim 1; *Amazon* Action Dkt.244-06 ('053 Patent) claim 1. As the Court's claim construction order makes clear, the term "repository" carries the same meaning in the Trusted Repository and Meta-rights Patents, respectively. *See Amazon* Action Dkt. 459 at 99.

C. The Importance of DRM

Individually and in combination, the patents-in-suit offer concrete technology solutions that address Barlow's "immense, unsolved conundrum." Ex. 3. In turn, these DRM solutions have catalyzed the creation of a whole new industry dedicated to the sale and distribution of digital content. As a senior member of the engineering team that developed the accused Apple FairPlay DRM technology, former Apple employee Rod Schultz, explained:

> Without DRM the iTunes store would never have been born. No music label would have licensed content to Apple, and the majority of the general public would not have purchased iTunes content that didn't come from a major label. . . .
>
> For video, DRM is even more important, and the studios can still set the rules without yielding to a public demand for DRM-free movies. When the cost of creating a movie like Avatar ranges between $300 million and $500 million, the studios naturally want their money back. They want protections in place that will give confidence to release digital copies to the world.

Ex. 4.

ContentGuard has successfully licensed the patents-in-suit, for substantial consideration, to companies around the world, including Casio, Fujitsu, Hitachi, LG Electronics, NEC, Nokia, Panasonic, Pantech, Sanyo, Sharp, Sony, Toshiba, and others. *Amazon* Action Dkt. 244 ¶ 39.

III. LEGAL PRINCIPLES

In Section 101, the Patent Act defines patentable subject matter: "Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title." 35 U.S.C. § 101. In drafting the Patent Act, "Congress took [a] permissive approach to patent eligibility to ensure that ingenuity should receive a liberal encouragement." *Bilski v. Kappos*, 561 U.S. 593, 601 (2010) (internal quotation marks omitted). That said, Section 101 does not encompass all products of human effort and ingenuity: laws of nature, physical phenomena, and abstract ideas are not patentable. *Diamond v. Chakrabarty*, 447 U.S. 303, 309 (1980).

In analyzing patent ineligibility challenges, courts "must distinguish between patents that claim the building blocks of human ingenuity and those that integrate the building blocks into something more, thereby transforming them into a patent-eligible invention." *Alice Corp.*, 134 S. Ct. at 2354. "On occasion, the Federal Circuit has described § 101 as a 'coarse eligibility filter"' to be applied *before* "the finer sieves" of Sections 102, 103, and 112 come into play. *Cal. Institute of Tech. v. Hughes Commcn's Inc.*, 2014 U.S. Dist. LEXIS 156763, *9 (C.D. Cal. Nov. 3, 2014) (quoting *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 1335, 1341, 1354 (Fed. Cir. 2013), *vacated sub nom.*, *WildTangent, Inc. v. Ultramercial, LLC*, 134 S. Ct. 2870 (2014)).

Courts evaluate challenges under Section 101 using a two-part test. First, a court must ask if the claim is "directed to one of those patent-ineligible concepts"—a law of nature, physical phenomenon, or abstract idea. *Alice Corp.*, 134 S. Ct. at 2355. Second, if it determines that the claim is directed to one of these concepts, the court must ask "[w]hat else is there in the claims before us?" *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 133 S. Ct. 1289, 1297 (2012).

"This second step determines whether there is an 'inventive concept' that 'ensure[s] that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.'" *Cal. Institute of Tech. v. Hughes Commcn's Inc.*, 2014 U.S. Dist. LEXIS 156763, *9 (citing *Alice Corp.*, 134 S. Ct. at 2355).

In *Alice Corp.*, the Supreme Court cautioned that courts should "tread carefully in construing th[e] exclusionary principle [of Section 101] lest it swallow all of patent law," noting that "at some level, all inventions . . . embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas." *Alice Corp.*, 134 S. Ct. at 2354 (citations and internal punctuation omitted). Thus, in the context of a Section 101 analysis, it is not appropriate to ignore the claims' *actual* limitations. "[A]ny claim can be stripped down, simplified, generalized, or paraphrased to remove all of its concrete limitations, until at its core, something that could be characterized as an abstract idea is revealed. [But a] court cannot go hunting for abstractions by ignoring the concrete, palpable, tangible limitations of the invention the patentee actually claims." *Ultramercial Inc.*, 772 F.3d at 1344. *See also Diamond v. Diehr*, 450 U.S. 175, 188 (1981) ("In determining the eligibility of respondent's claimed process for patent protection under section 101, the[] claims must be considered as a whole.").

IV. ARGUMENT

All the DRM inventions taught by the patents-in-suit are eligible for patent protection. Far from "merely recit[ing] the performance of some business practice known from the pre-Internet world along with the requirement to perform it on the Internet," *DDR Holdings, LLC v. Hotels.com, L.P.*, 2014 U.S. App. LEXIS 22902, *26 (Fed. Cir. Dec. 5, 2014), each of ContentGuard's patents teaches concrete, innovative solutions that address the challenge of protecting and distributing digital content in the advent of the Internet.

A. The Trusted Repository Patents Are Eligible for Patent Protection.

1. The Trusted Repository Patents Do Not Disclose "Abstract Ideas."

Defendants spend 21 pages of their motion attempting to line up the myriad elements of the asserted claims with alleged "corresponding action[s]" purportedly existing in bricks-and-mortar libraries. *Amazon* Action Dkt. 539 at 7-28. According to Defendants, this exercise demonstrates that the Trusted Repository Patents cover "nothing more than . . . [a] basic library loan concept" implemented by "generic computer hardware and software." *Id.* at 1. These assertions are meritless.

First, Defendants' arguments are premised on the assertion that "ContentGuard's patents specify nothing beyond using generic computer hardware and software to perform the basic functions of a computer—secure storage, encrypted transmission of data, and reliable execution of instructions—to enforce usage rights and restrictions, just as librarians have done with pen and paper for hundreds of years." *Amazon* Action Dkt. 539 at 1 (emphasis added). But merely stating Defendants' hypothesis exposes its fatal flaws. Nowhere do Defendants explain how a bricks-and-mortar library, coupled with a generic computer, meets the three "integrities" taught by the Trusted Repository Patents.

- "*Physical integrity.*" Defendants assert that a "library 'prevent[s] access to information' in its possession by non-trusted persons by, among other things, locking its doors, installing security gates at its entrances and exits and requiring patrons to present valid library cards in order to formally check out materials." *Amazon* Action Dkt. 539 at 10. But the "physical" integrity taught by the Trusted Repository Patents is *not the same* as locking a door or installing a gate. Moreover, even if Defendants had adequately explained how a library's walls and gates amount to "physical integrity" within the meaning of the Trusted Repository Patents, those patents also require that the computing device *receiving* digital

content also maintain "physical integrity." Defendants point to nothing in the library setting that establishes the library patron's "physical integrity."[5]

- "*Communications integrity*." Defendants assert that "a library maintains communications integrity by lending materials only to patrons who 'are able to present proof that they are trusted' in the form of a valid library card—if a patron cannot present a library card, he or she cannot borrow a book or DVD." *Amazon* Action Dkt. 539 at 11. But the "communications integrity" taught by the Trusted Repository Patents is *not the* same as an interaction with a patron in a library setting. A "library card" is merely proof of the possessor's identity; it is not a guarantee that he or she can safely receive valuable digital content and be *prevented* from misusing it once access is conveyed.
- "*Behavioral integrity*." Defendants assert that (1) "a library will maintain a database of authorized patrons and will issue to each of those patrons a 'certificate' (in the form of a library card) that attests to his or her status as an authorized and trusted borrower" and (2) "a library will conduct a background/reference check of any person applying for a position as a librarian; as part of this process, the applicant will have to show proof of identity—a 'certificate' in the form of a driver's license, passport or other government issued ID." *Amazon* Action Dkt. 539 at 11-12." How these "background checks" are equivalent to what the Trusted Repository Patents calls "behavioral integrity"—*i.e.*, "requiring software to include a digital certificate in order to be installed in the repository" (*Amazon* Action Dkt. 459 at 21)—is a complete mystery.

[5] In its motion for judgment on the pleadings, Google took the position that because library patrons are able to physically "*hold* and store a book," *i.e.*, through use of parts of human anatomy, a briefcase, etc., library patrons also maintain "physical integrity." *Cf. Google* Action Dkt. 137 at 11-12 n.5 (emphasis added). Defendants appear to have abandoned this facially untenable position.

At bottom, Defendants have concocted a far-fetched "analogy to conventional [practices, but that] is no substitute for an analysis of how, or why, the claim language supports [the] assertion that the claims merely recite [an allegedly] abstract [conventional practice]."[6] Defendants' inability to demonstrate how and why the actual claims of Trusted Repository Patents meaningfully resemble a trip to the library is fatal. *SimpleAir, Inc.*, Ex. 14 at 16 ("[E]very method can be generalized to the point of abstraction if the claim language is ignored. Here, Petitioner overlooks the various physical components recited by the claims . . . [and] Petitioner's analogy to conventional periodical publication delivery still fails because it does not account for each step of the claimed method. . . . Petitioner's generalized arguments, not directed to the specific language of the challenged claims, are insufficient to show that the claims more likely than not are directed to a patent-ineligible abstract idea."); *Ultramercial Inc.*, 772 F.3d at 1344 ("[A]ny claim can be stripped down, simplified, generalized, or paraphrased to remove all of its concrete limitations, until at its core, something that could be characterized as an abstract idea is revealed. [But a] court cannot go hunting for abstractions by ignoring the concrete, palpable, tangible limitations of the invention the patentee actually claims.").

Second, what Defendants are really telling the Court is that a novel, concrete, technology-based solution for ensuring the integrity of content-distribution systems and of usage rights associated with the content being distributed is analogous to an honor-based code practiced for centuries by libraries and their patrons, *e.g.*, "I pledge not to copy and will return the book after 7 days."[7] That assertion also does not pass the straight-face test. Indeed, Defendants have it *exactly backwards*. That is, Stefik and his colleagues saw past an *abstract*, unenforceable idea of "trust" that was plainly unsuitable to protect digital-distribution systems in the advent of a new

[6] *See Google Inc. v. SimpleAir, Inc.*, Case CBM2014-00170, Slip op. at 15 (U.S. Patent Trial & Appeal Board, Jan. 22, 2015), attached hereto as Ex. 14.

[7] *See, e.g.*, *Amazon* Action Dkt. 539 at 25 (equating "the server mode of operation is operative to enforce usage rights associated with content . . ." with "[w]hen the patron obtains the book, CD or video from the library, he agrees to and does use the book only in accordance with the library's specified rules . . .").

medium acknowledged as a "pirate's paradise" (Ex. 5), and replaced it with a comprehensive, technology-based solution that solved what Barlow coined as "the problem of digitized property" (Ex. 3).

It is important to note that preventing the unauthorized copying and distribution of digital content presents altogether different challenges from those that surround the protection of content existing in physical form, *e.g.*, printed books. To protect printed matter, libraries rely for the most part on an honor code—the patron "agrees" to not copy the book and return it on the stipulated date. And while the library may impose financial penalties to guard against the theft or late return of a book, *e.g.*, a late $0.15 per day (*see* Ex. 12), once the book has left the premises there is nothing the library can do to *actually* guard against its theft, unauthorized copying,[8] or further lending. Once the content is digital, however, the challenges of protecting it are far more complex and the stakes are infinitely higher. An honor code will simply not do. As Karen Coyle, an expert in library technologies, has explained:

> [L]et's say that I have the very same book in a digital format. If I want to make a copy, I can make that copy almost instantly. It will cost me nothing. And the end result will be a perfect copy of the original. Not only that, I can make one hundred or a thousand copies almost as easily as I can make one. I can email the file to everyone in my address book, or I can place the file on a peer-to-peer network and let anyone on the Internet have access to it. With the digital file, the economics are slanted very much toward making copies.
>
> Note that the digital file is protected by the very same copyright law that the hard copy is, the one that doesn't really prevent us from making copies. What we have here is the Napster effect, which is based on the ease of copying. And because law doesn't seem to have worked as a preventive measure, there is some

[8] In the library setting, an honor code may suffice because, given the economics involved, it makes little sense for the patron to engage in wholesale unauthorized copying. *See* Ex. 13 ("Say I have a book, a hard copy book, that I have borrowed from the library. Maybe I would like to have a copy of my own. . . . Yet I am unlikely to copy the book. Why is that? Because I don't want to spend an hour and a half at a copy center opening the pages and punching the copy button. Because in the end the copy will cost me as much or more than buying a copy of the book in paperback. And because what I will end up with is a poor copy on bad paper in an 8.5x11 format, unbound. In the end, making a copy of a hard copy books is uneconomical, in terms of time and money, and the result is pretty undesirable.").

> justification that *only a technology-based protection will ever work to protect digital works*.

Ex. 13 (emphasis added).

Thus, rather than "merely recite the performance of some business practice known from the pre-Internet world along with the requirement to perform it on the Internet," *DDR Holdings, LLC*, 2014 U.S. App. LEXIS 22902, *26, the Trusted Repository Patents disclose precisely the type of "technology-based" solutions Coyle had in mind. Using Stefik's Trusted Repository Patents, an online digital content distributor (like iTunes or Google Play) can *effectively prevent* the theft, unauthorized use, copying, or further distribution of content. By way of example, (i) a customer who has paid for the right to watch the content only once can be prevented from watching it again; (ii) a customer who has paid for the right to watch the content on a particular device (*e.g.*, a tablet) can be prevented from watching it on a different device (*e.g.*, a high-definition TV); (iii) a customer who has paid for the right to watch the content for 24 hours can be prevented from watching it upon the expiry of the specified rental period, and so on and so forth. All of these "usage rights" restrictions are *enabled* and *effectively enforced* using the "technology-based" teachings of Stefik's Trusted Repository Patents. In contrast, however, *none* can be accomplished in the library setting, and thus, to see their books returned on time and in the same condition in which they left, libraries must rely solely on their patron's unenforceable promises. And, to be sure, solutions of the type disclosed in Trusted Repository Patents, which are grounded in *technology* and yield *tangible results*, are the opposite of abstraction.

Third, Defendants' assertions that the Trusted Repository Patents require nothing more than the "use of generic computer system and generic computer concepts" (*Amazon* Action Dkt. 539 at 24) are flatly incorrect. In truth, Stefik's Trusted Repository Patents teach that "trusted systems . . . [are] the only feasible way to implement digital rights management *because general-purpose computers* have too many security holes." Ex. 6 (emphasis added). And there is *zero*

proof in the record that a "generic computer" maintains the three integrities taught by the Trusted Repository Patents.[9]

Fourth, after three rounds of briefing, Defendants appear to have expressly abandoned all of their preemption arguments. *Compare Google* Action Dkt. 137 at 2 (asserting that the Trusted Repository Patents stake a claim to "the entire abstract idea of imposing and enforcing usage rights and restrictions on digital content"). This is significant because it underscores that the subject matter of the Trusted Repository Patents is narrow, *i.e.*, limited to devices that maintain physical, communications, and behavioral integrity, rather than *all* devices that are capable to receive content via the Internet. ContentGuard's inventions are thus "inherently limited to the sphere of application rather than abstraction." *Rockstar Consortium US LP, Inc. v. Samsung Elecs. Co., Ltd.*, 2014 U.S. Dist. LEXIS 67097, at *15 (E.D. Tex. May 15, 2014) (Gilstrap, J.). This Court's precedent is clear that patents that "clearly articulate a process that is meaningfully limited" are not abstract and fall outside the scope of Section 101. *Id.* at *16.[10]

2. The Trusted Repository Patents Teach Inventive Concepts.

Even if Defendants were correct (and they are not) that the Trusted Repository Patents concern "abstract ideas," the limitations taught by the asserted claims are inventive and involve

[9] Defendants assert that "the Stefik patent specification makes clear that the integrities/'security levels' for a 'trusted' system (which the specification also calls a 'repository') are not even fixed or specifically defined." *Amazon* Action Dkt. 539 at 10. This argument appears to be a refinement of an argument previously urged by Google and Motorola, that the specification includes "repositories . . . with virtually no security whatsoever." *Google* Action Dkt. 137 at 13. As ContentGuard explained in its responsive pleading to Google and Motorola's previous motions, however, this argument was rejected by the PTAB during the recently concluded IPRs as "directly contrary to the meaning of 'repository' as defined in the glossary." Ex. 11 at 12.

[10] Defendants' reliance on this Court's recent decision in *Clear with Computers LLC v. Altec Industries, Inc.*, No. 6:14-cv-79, Slip Op. at 7 (E.D. Tex. Mar. 3, 2015), is misplaced. The patents at issue in that case, which were directed to the idea of "creating a customized sales proposal for a customer," *see id.* at 6, have nothing meaningful in common with the Trusted Repository or Meta-rights patents at issue in this litigation. For the same reasons, the scores of cases Defendants cite in a footnote of their motion (*see Amazon* Action Dkt. 539 at 3 n.1), are also inapposite.

meaningful limitations that cover much more than "well-understood, routine, [or] conventional activity." *See Mayo Collaborative Servs.*, 132 S. Ct. at 1298.

First, the three integrities required to implement a "trusted repository" are not merely the routine or conventional use of a general-purpose computer. "Prevent[ing] access to information by a non-trusted system," so as to implement "physical integrity," is no routine business activity, and Defendants have not proven otherwise. Nor is ensuring that the recipient computing device implements "communications integrity" by "only communicat[ing] with other devices that are able to present proof that they are trusted systems, for example, by using security measures such as encryption, exchange of digital certificates, and nonces."[11] Finally, implementing "behavioral integrity" by "requiring software to include a digital certificate in order to be installed in the repository" is also not a routine, conventional business activity. To the contrary, individually and in combination, the requirement that these integrities be implemented are precisely the type of "inventive concept" that can render an otherwise "abstract idea" patentable. *See DDR Holdings, LLC*, 2014 U.S. App. LEXIS 22902, *31 (holding that claims that do not "recite a commonplace business method aimed at processing business information, applying a known business process to the particular technological environment of the Internet, or creating or altering contractual relations using generic computer functions and conventional network operations, such as the claims in *Alice*, *Ultramercial*, *buySAFE*, *Accenture*, and *Bancorp* . . . [are] patent-eligible under § 101").

Second, there is no evidence in the record that the "trusted repository" inventions taught by the Stefik patents are a feat of "routine," "prosaic" engineering, such that they are devoid of

[11] Defendants argue that the patents teach the use of various "conventional" techniques. Even if true, this assertion is beside the point. "On a fundamental level, the creation of new compositions and products based on combining elements from different sources has long been a basis for patentable inventions." *DDR Holdings, LLC*, 2014 U.S. App. LEXIS 22902, *28 n.5 (citing *Parks v. Booth*, 102 U.S. 96, 102 (1880) ("Modern inventions very often consist merely of a new combination of old elements or devices, whether nothing is or can be claimed except the new combination.")).

an "inventive" concept.[12] *See DDR Holdings, LLC*, 2014 U.S. App. LEXIS 22902, *30 (holding that a patent "that overrides the routine" does not run afoul of *Alice Corp.*); *Vanderbilt Univ. v. ICOS Corp.*, 601 F.3d 1297, 1302 (Fed. Cir. 2010). To the contrary, all the evidence in the record compels the opposite conclusion: that Stefik's Trusted Repository Patents are one of the seminal "development[s] that catalyzed the DRM paradigm" (Ex. 6), and a novel technical solution to a problem previously thought to be "immense" and "unsolved" (Ex. 3). Indeed, experts in library technologies have noted that "trusted systems" are "sophisticated technology" and, as of 2003, *i.e.*, nearly 10 years after Stefik and his colleagues conceived the Trusted Repository Patents, the "development of trusted systems [was still] occupying the attention of computer scientists." Ex. 13.

Third, the inventiveness of the "trusted" repository concepts taught by the Trusted Repository Patents is underscored by the PTAB's recent decisions reaffirming the validity of four of these patents. As noted, the '859, '576, '072, and '160 Patents were recently challenged before the PTAB in *Inter Partes* reviews. Ex. 9. The PTAB, however, reaffirmed the validity of each and every claim of the '859, '576, and '072 Patents, and altogether refused to institute a review of the asserted claims of the '160 Patent. The principal basis for the PTAB's decisions was its conclusion that the challenger's asserted prior art did not disclose Stefik's "repository" limitations—a limitation that is present in all asserted claims. Ex. 11. If Defendants were correct that a "repository" is nothing more than a general-purpose computer that implements an abstract idea, the PTAB would not have affirmed the '859, '576, and '072 Patents' validity or declined to institute a review of the asserted claims of the '160 Patent. Given the PTAB's long

[12] In cases involving inventorship disputes, the Federal Circuit has made it clear that the threshold for "inventiveness" is satisfied when, among other things, an inventor makes a contribution that is "not insignificant in quality" and goes beyond "well-known concepts and/or the current state of the art." *Pannu v. Iolab Corp.*, 155 F.3d 1344, 1351 (Fed. Cir. 1998). The Federal Circuit has also made clear that the threshold of "inventiveness" is not very high. *Mintz v. Dietz & Watson, Inc.*, 679 F.3d 1372, 1377 (Fed. Cir. 2012) ("Often the inventive contribution lies in defining the problem in a new revelatory way.").

track record of invalidating patents, it would defy logic to conclude otherwise, particularly given that the art the challenger put before the PTAB involved "computers." *See* Ex. 11 at 20 ("Leroux discloses a method of acquiring software programs by microcomputers"). The PTAB's decision to firmly go against the tide in the case of the Stefik Trusted Repository Patents is dispositive of Defendants' arguments here.

Fourth, the "inventiveness" of the "trusted" system limitation taught by the Stefik patents is reinforced by the numerous "objective indicia of non-obviousness" that exist here.[13] The Stefik Trusted Repository Patents are no ordinary patents. They rest upon "pioneering" work that has received numerous accolades. Ex. 7. They were conceived in the face of enormous skepticism and solved what leading commentators considered an "immense, unsolved conundrum." Ex. 3, 5. "Trusted" systems are now firmly considered a "core technolog[y] that underlie[s] . . . technological protection systems" (Ex. 7), and Stefik is "acknowledged [as the] father of DRM" (Ex. 1). Stefik's Trusted Repository Patents have been praised as disclosing fundamental technology "*necessary* to make the digital delivery of music, movies and other files secure." Ex. 8 (emphasis added). Indeed, the fundamental nature of the Trusted Repository Patents prompted the EU antitrust authorities to threaten legal action against Microsoft out of concern that it could use the patents to become a monopolist in the market for DRM technologies. Ex. 2. ContentGuard has successfully licensed the Stefik Trusted Repository Patents, for substantial consideration, to scores of companies. Dkt. 244 ¶ 39. Finally, Stefik's vision concerning the role "trusted" systems must play in the distribution of digital content over

[13] ContentGuard does not mean to suggest that it would be appropriate for the Court to conduct a validity analysis in the context of this motion, let alone that the presence or absence of objective indicia of non-obviousness should be a litmus test for determining patent eligibility. However, as Federal Circuit Judge Jimmy Reyna recently noted, "courts handling patent infringement matters [should] treat evidence corresponding to the factors identified in *Graham* as strong, if not the best, evidence of innovation—i.e., the manner in which the industry and the marketplace responded to the disclosure in a patent." *Apple Inc. v. ITC*, 725 F.3d 1356, 1375 (Fed. Cir. 2013) (Reyna, J., concurring in part and dissenting in part).

the internet is one of the seminal "development[s] that catalyzed the DRM paradigm" (Ex. 6) and created an entirely new industry that has benefitted Defendants to the tune of billions of dollars.

Fifth, even if the "repository"/"trusted" system limitation taught by the Trusted Repository Patents were not inventive by itself (and it plainly is), Defendants' motion still fails because Defendants have not demonstrated that the patents are devoid of inventiveness "as an ordered combination" when considered alongside other limitations recited by the claims. *Cal. Institute of Tech.*, 2014 U.S. Dist. LEXIS 156763, *10. "When viewing claim elements as an ordered combination, the court should not ignore the presence of *any* element, even if the element, viewed separately, is abstract. If the ordered combination of elements constitutes conventional activity, the claim is not patentable, but courts should remember that a series of conventional elements may together form an unconventional, patentable combination." *Cal. Institute of Tech.*, 2014 U.S. Dist. LEXIS 156763, *10-11; *see also DDR Holdings, LLC*, 2014 U.S. App. LEXIS 22902, *28 n.5 ("[o]n a fundamental level, the creation of new compositions and products based on combining elements from different sources has long been a basis for patentable inventions.") (citations omitted). While they attempt to dissect and deconstruct the claims element by element, Defendants never address the entire "ordered combinations" taught by the Trusted Repository Patents. Nor Defendants prove that, as a matter of law, those "ordered combinations" are not eligible for patent protection.

B. The Meta-rights Patents Are Eligible for Patent Protection.

1. The Meta-rights Patents Do Not Disclose "Abstract Ideas."

The crux of Defendants' patent ineligibility attacks with respect to the Meta-rights Patents is the assertion that both patents recite an "idea" that "can be (and has been historically) implemented using written agreements and over-the-counter transactions." *Amazon* Action Dkt. 539 at 30-31. Defendants are mistaken for several reasons.

First, contrary to Defendants contention, these patents teach much more than an "idea" that has existed in "over-the-counter" commerce for quite some time. *Cf. id.* The patents in fact

claim "meta-rights" that are "*enforceable by a repository*." *See Amazon* Action Dkt. 244-05 ('280 Patent) claim 1; Dkt. 255-06 ('053 Patent) claim 1 (emphasis added). To quote Apple's own counsel, who spoke on behalf of all Defendants during the *Markman* hearing,[14] "that is very important" because within the context of the actual claims "a meta-right" is "*not something that is abstract or generalized*, but [rather something that] is used by a repository." Ex. 15 at 125:6-10 (emphasis added). Defendants' unambiguous admission that "meta-rights" that are "used by a repository" are "*not something that is abstract or generalized*" dooms Defendants' motion.[15]

Second, Defendants' suggestion that the inventions taught by the '280 and '053 Patents can be implemented using written agreements (*cf. Amazon* Action Dkt. 539 at 30-31) is demonstrably false, and fails for the same reason as Defendants' flawed "library" analogy discussed above. *See supra* at 9-12. Interactions undertaken via "written agreements and traditional mail" simply lack the three integrities required by a trusted "repository," and Defendants fail to show otherwise. Moreover, the Meta-rights Patents specifically disclose and claim "state variable" elements that are used to track and control the exercise of created rights, further removing these patents from the realm of patent-ineligible ideas. At bottom, the mode of analysis proposed by Defendants is "unhelpful for computer inventions. Many inventions could be theorized with pencil and paper, but pencil and paper can rarely produce the actual effect of the invention. Likewise, with regard to software, a human could spend months or years writing on paper the 1s and 0s comprising a computer program and applying the same algorithms as the program. At the end of the effort, he would be left with a lot of paper that obviously would not produce the same result as the software." *Cal. Inst. of Tech.*, 2014 U.S. Dist. LEXIS 156763, at *49.

[14] Counsel for Apple's co-Defendants did not disavow these statements during the hearing, nor did counsel give any indication that counsel for Apple was not authorized to speak on behalf of the entire defense group. Moreover, counsel for Apple spoke in response to the Court's request to "hear from the Defendants." Ex. 15 at 124:17-21.

[15] Defendants' attempt to explain away these admissions in a footnote (*Amazon* Action Dkt. 539 at 30 n.15) does not pass muster.

Third, Defendants raise no credible preemption arguments with respect to the Meta-rights Patents, nor could they. Like the Stefik Trusted Repository Patents, the Meta-rights Patents are "inherently limited to the sphere of application rather than abstraction." *Rockstar Consortium US LP*, 2014 U.S. Dist. LEXIS 67097, at *15. That is, the inventions are limited to the use of "meta-rights" enforceable by devices that maintain physical, communications, and behavioral integrity, rather than *all* devices that are capable of receiving content via the Internet. Further, the meta-rights contemplated by the '280 and '053 Patents are limited to "rights that one has to generate, manipulate, modify, dispose of or otherwise derive other rights" *but* without resulting in "actions to content." *Amazon* Action Dkt. 244-05 ('280 Patent) at col. 5:45-47, 7:26-31.

2. The Meta-rights Patents Teach Inventive Concepts.

Even if Defendants were correct (and they are not) that the Meta-rights Patents concern "abstract ideas," the asserted claims teach inventive, meaningful limitations that cover much more than "well-understood, routine, [or] conventional activity." *See Mayo Collaborative Servs.*, 132 S. Ct. at 1298.

The combination of, among other things, "meta-rights," trusted "repositor[ies]," and "state variable[s]" taught by the claims is precisely the type of "inventive concept" that can render an otherwise "abstract idea" patentable. *See DDR Holdings, LLC*, 2014 U.S. App. LEXIS 22902, *31 (holding that claims that do not "recite a commonplace business method aimed at processing business information, applying a known business process to the particular technological environment of the Internet, or creating or altering contractual relations using generic computer functions and conventional network operations, such as the claims in *Alice*, *Ultramercial*, *buySAFE*, *Accenture*, and *Bancorp* . . . [are] patent-eligible under § 101"). There is no evidence in the record that the combination of "meta-rights," trusted "repositor[ies]," and "state variable[s]" are a feat of "routine," "prosaic" engineering, such that they are devoid of an "inventive" concept, and Defendants do nothing to prove that the claims are ineligible for patent protection "as an ordered combination." *Cal. Institute of Tech.*, 2014 U.S. Dist. LEXIS 156763,

*10. While Defendants assert—without support—that there is nothing "inventive" about any element recited by the claims, "courts should remember that a series of conventional elements may together form an unconventional, patentable combination." *Cal. Institute of Tech.*, 2014 U.S. Dist. LEXIS 156763, *10-11; *see also DDR Holdings, LLC*, 2014 U.S. App. LEXIS 22902, *28 n.5 ("[o]n a fundamental level, the creation of new compositions and products based on combining elements from different sources has long been a basis for patentable inventions.") (citations omitted).

V. CONCLUSION

For the foregoing reasons, Defendants' motion should be denied.

Dated: May 11, 2015

Respectfully submitted,

/s/ Sam Baxter

Samuel F. Baxter
Texas State Bar No. 01938000
sbaxter@mckoolsmith.com
MCKOOL SMITH P.C.
104 East Houston, Suite 300
Marshall, Texas 75670
Telephone: (903) 923-9000
Facsimile: (903) 923-9099

Robert A. Cote
rcote@mckoolsmith.com
John C. Briody
jbriody@mckoolsmith.com
Radu A. Lelutiu
rlelutiu@mckoolsmith.com
Shahar Harel
sharel@mckoolsmith.com
David R. Dehoney
ddehoney@mckoolsmith.com
Dana E. Vallera
dvallera@mckoolsmith.com
Angela M. Vorpahl
avorpahl@mckoolsmith.com
MCKOOL SMITH P.C.
One Bryant Park, 47th Floor
New York, New York 10036
Telephone: (212) 402-9400
Facsimile: (212) 402-9444

Holly E. Engelmann
hengelmann@mckoolsmith.com
Seth R. Hasenour
shasenour@mckoolsmith.com
Eric S. Hansen
ehansen@mckoolsmith.com
MCKOOL SMITH P.C.
300 Crescent Court, Suite 1500
Dallas, Texas 75201
Telephone: (214) 978-4000
Facsimile: (214) 978-4004

ATTORNEYS FOR CONTENTGUARD HOLDINGS, INC.

CERTIFICATE OF SERVICE

The undersigned certifies that the foregoing document was filed electronically in compliance with Local Rule CV-5(a). As such, this document was served on all counsel who have consented to electronic services on this the 11th day of May, 2015. Local Rule CV-5(a)(3)(A).

/s/ Radu A. Lelutiu